
	<b>COUNTY OF SAN BERNARDINO</b>  <b>POLICY</b>	No. 2-360 Effective: February 6, 2006 By: Bea Valdez, Interim Chief of Administrative Services  Issue No. 1 Page 1 of 2
	<b>PUBLIC HEALTH</b>	Approved:  James A. Felten Public Health Director
Subject: DEVICE AND MEDIA CONTROLS		

#### **I. POLICY:**

It is the policy of the Department of Public Health (DPH) to protect its systems and all sensitive (confidential, restricted or protected) information, which resides on technology devices and/or removable media and to ensure that safeguards are in place to govern the use of such technology. Devices and media that may contain sensitive information need to be controlled to ensure data integrity, confidentiality, and security.

#### **II. PURPOSE:**

The purpose of this policy is to establish guidelines for DPH workforce members for the handling of devices and media that may contain sensitive information.

#### **III. GENERAL INFORMATION:**

Media can be any device or medium that is used to store sensitive information.

Devices covered under this policy include but are not limited to:

- Laptops
- Personal Digital Assistants
- Hard drives
- Storage systems
- Floppy disks
- CD ROMs
- Memory sticks
- Wireless devices
- Magnetic tapes
- Blackberries
- Cell phones
- Handheld devices

#### **IV. PROCEDURE:**

##### **A. Use of Storage Media**

1. Any use of removable media to store or transport sensitive information is discouraged, unless approved by the program manager.
2. Any storage device or removable media that has been authorized to contain sensitive information must be properly secured in a locked location with limited access when not in use.
3. Each program is required to document the movement of sensitive information and ensure that appropriate safeguards are in place to protect the sensitive information.

##### **B. Destruction or Re-Use of Media Storage Devices**

Prior to destroying or re-using any storage device or removable media, the user must ensure that the device or media does not contain sensitive information.

1. If the device or media contains sensitive information that should be preserved, make a backup copy.
2. If the device or media contains sensitive information that is not needed, consult with Information Technology on proper disposal.
3. If removable media is to be re-used for the purpose of system backups and disaster recovery, and the media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

**V. VIOLATIONS:**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment/contract.

**VI. REFERENCE:**

A. Reference

- Health Insurance Portability and Accountability Act Code of Federal Regulations (CFR) Parts 160 and 164

B. Citations

1. §164.310(d)(1) – Standard – Device and Media Controls
2. §164.310(d)(2)(i) – Disposal – Device and Media Controls
3. §164.310(d)(2)(ii) – Media re-use – Device and Media Controls
4. §164.310(d)(2)(iii) – Accountability – Device and Media Controls
5. §164.310(d)(2)(iv) – Data backup and storage – Device and Media Controls